

WHAT IS CLAIMED IS:

1. A method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:

(a) receiving an encrypted media encryption key at the host receiver;
5 (b) decrypting the encrypted media encryption key at the host receiver;
(c) re-encrypting the decrypted media encryption key at the host receiver using a pairing key;

(d) transferring the re-encrypted media encryption key from the host receiver to the client receiver;

10 (e) decrypting the re-encrypted media encryption key at the client receiver using the pairing key;

(f) receiving encrypted program materials from the broadcast system at the host receiver;

(g) transferring the encrypted program materials from the host receiver to the
15 client receiver; and

(h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.

2. The method of claim 1, further comprising decrypting the encrypted
20 program materials at the host receiver using the decrypted media encryption key.

3. The method of claim 1, further comprising receiving the pairing key from the broadcast system at both the host receiver and the client receiver.

25 4. The method of claim 3, wherein the receiving step comprises:
receiving the pairing key from the broadcast system at the host receiver, wherein the pairing key is encrypted; and

decrypting the pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

30 5. The method of claim 3, wherein the receiving step comprises:

receiving the pairing key at the client receiver, wherein the pairing key is encrypted; and

decrypting the pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

5

6. The method of claim 5, further comprising:

receiving the pairing key from the broadcast system at the host receiver; and
transferring the pairing key from the host receiver to the client receiver.

10

7. An apparatus for distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:

(a) means for receiving an encrypted media encryption key at the host receiver;
(b) means for decrypting the encrypted media encryption key at the host receiver;
(c) means for re-encrypting the decrypted media encryption key at the host

15

receiver using a pairing key;

(d) means for transferring the re-encrypted media encryption key from the host receiver to the client receiver;

(e) means for decrypting the re-encrypted media encryption key at the client receiver using the pairing key;

20

(f) means for receiving encrypted program materials from the broadcast system at the host receiver;

(g) means for transferring the encrypted program materials from the host receiver to the client receiver; and

25

(h) means for decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.

30

8. The apparatus of claim 7, further comprising means for decrypting the encrypted program materials at the host receiver using the decrypted media encryption key.

9. The apparatus of claim 7, further comprising means for receiving the pairing key from the broadcast system at both the host receiver and the client receiver.

10. The apparatus of claim 9, wherein the means for receiving comprises:
5 means for receiving the pairing key from the broadcast system at the host receiver, wherein the pairing key is encrypted; and
means for decrypting the pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

10 11. The apparatus of claim 9, wherein the means for receiving comprises:
means for receiving the pairing key at the client receiver, wherein the pairing key is encrypted; and
means for decrypting the pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

15 12. The apparatus of claim 11, further comprising:
means for receiving the pairing key from the broadcast system at the host receiver;
and
means for transferring the pairing key from the host receiver to the client receiver.

20 13. A method of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:

(a) receiving an encrypted media encryption key at a conditional access module associated with the host receiver;

25 (b) decrypting the encrypted media encryption key at the conditional access module;

(c) re-encrypting the decrypted media encryption key at the conditional access module using a first pairing key shared between the conditional access module and the host receiver;

30 (d) transferring the re-encrypted media encryption key from the conditional access module to the host receiver;

(e) receiving the re-encrypted media encryption key at the host receiver from the conditional access module;

(f) decrypting the re-encrypted media encryption key at the host receiver using the first pairing key shared between the conditional access module and host receiver;

5 (g) re-encrypting the decrypted media encryption key at the host receiver using a second pairing key shared between the host receiver and the client receiver;

(h) transferring the re-encrypted media encryption key from the host receiver to the client receiver; and

10 (i) decrypting the re-encrypted media encryption key at the client receiver using the second pairing key shared between the host receiver and the client receiver;

(j) receiving encrypted program materials from the broadcast system at the host receiver;

(k) transferring encrypted program materials from the host receiver to the client receiver; and

15 (l) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.

14. The method of claim 13, further comprising decrypting the encrypted program materials received from the broadcast system at the host receiver using the
20 decrypted media encryption key.

15. The method of claim 13, further comprising receiving the first pairing key from the broadcast system at both the host receiver and the conditional access module.

25 16. The method of claim 15, wherein the receiving step comprises: receiving the first pairing key from the broadcast system at the host receiver, wherein the first pairing key is encrypted; and

decrypting the first pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

30

17. The method of claim 15, wherein the receiving step comprises:

receiving the first pairing key from the broadcast system at the conditional access module; and
decrypting the first pairing key at the conditional access module.

5 18. The method of claim 13, further comprising receiving the second pairing key from the broadcast system at both the host receiver and the client receiver.

 19. The method of claim 18, wherein the receiving step comprises:
 receiving the second pairing key from the broadcast system at the host receiver,
10 wherein the second pairing key is encrypted; and
 decrypting the second pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

 20. The method of claim 18, wherein the receiving step comprises:
15 receiving the second pairing key at the client receiver, wherein the second pairing key is encrypted; and
 decrypting the second pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

20 21. The method of claim 20, further comprising:
 receiving the second pairing key from the broadcast system at the host receiver;
 and
 transferring the second pairing key from the host receiver to the client receiver.

25 22. An apparatus for distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:
 (a) means for receiving an encrypted media encryption key at a conditional access module associated with the host receiver;
 (b) means for decrypting the encrypted media encryption key at the conditional
30 access module;

(c) means for re-encrypting the decrypted media encryption key at the conditional access module using a first pairing key shared between the conditional access module and the host receiver;

5 (d) means for transferring the re-encrypted media encryption key from the conditional access module to the host receiver;

(e) means for receiving the re-encrypted media encryption key at the host receiver from the conditional access module;

10 (f) means for decrypting the re-encrypted media encryption key at the host receiver using the first pairing key shared between the conditional access module and host receiver;

(g) means for re-encrypting the decrypted media encryption key at the host receiver using a second pairing key shared between the host receiver and the client receiver;

15 (h) means for transferring the re-encrypted media encryption key from the host receiver to the client receiver; and

(i) means for decrypting the re-encrypted media encryption key at the client receiver using the second pairing key shared between the host receiver and the client receiver;

20 (j) means for receiving encrypted program materials from the broadcast system at the host receiver;

(k) means for transferring encrypted program materials from the host receiver to the client receiver; and

25 (l) means for decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.

23. The apparatus of claim 22, further comprising means for decrypting the encrypted program materials received from the broadcast system at the host receiver using the decrypted media encryption key.

24. The apparatus of claim 22, further comprising means for receiving the first pairing key from the broadcast system at both the host receiver and the conditional access module.

5 25. The apparatus of claim 24, wherein the means for receiving comprises:
means for receiving the first pairing key from the broadcast system at the host receiver, wherein the first pairing key is encrypted; and
means for decrypting the first pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

10 26. The apparatus of claim 24, wherein the means for receiving comprises:
means for receiving the first pairing key from the broadcast system at the conditional access module; and
means for decrypting the first pairing key at the conditional access module.

15 27. The apparatus of claim 22, further comprising means for receiving the second pairing key from the broadcast system at both the host receiver and the client receiver.

20 28. The apparatus of claim 27, wherein the means for receiving comprises:
means for receiving the second pairing key from the broadcast system at the host receiver, wherein the second pairing key is encrypted; and
means for decrypting the second pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

25 29. The apparatus of claim 27, wherein the means for receiving comprises:
means for receiving the second pairing key at the client receiver, wherein the second pairing key is encrypted; and
means for decrypting the second pairing key at the client receiver using a receiver
30 key uniquely associated with the client receiver.

30. The apparatus of claim 29, further comprising:
means for receiving the second pairing key from the broadcast system at the host
receiver; and
means for transferring the second pairing key from the host receiver to the client
5 receiver.

31. A method of distributing program materials received from a broadcast
system between a host and client receiver for remote decryption, comprising:
(a) receiving an encrypted media encryption key at a conditional access module
10 associated with the host receiver;
(b) decrypting the encrypted media encryption key at the conditional access
module;
(c) re-encrypting the decrypted media encryption key at the conditional access
module using a pairing key shared between the conditional access module and the client
15 receiver;
(d) transferring the re-encrypted media encryption key from the conditional access
module to the client receiver;
(e) decrypting the re-encrypted media encryption key at the client receiver using
the pairing key shared between the conditional access module and client receiver;
20 (f) receiving encrypted program materials from the broadcast system at the host
receiver;
(g) transferring encrypted program materials from the host receiver to the client
receiver; and
(h) decrypting the encrypted program materials at the client receiver using the
25 decrypted media encryption key.

32. The method of claim 31, further comprising receiving the pairing key from
the broadcast system at both the conditional access module and the client receiver.

30 33. The method of claim 32, wherein the receiving step comprises:

receiving the pairing key from the broadcast system at the conditional access module, wherein the pairing key is encrypted; and
decrypting the pairing key at the conditional access module.

5 34. The method of claim 32, wherein the receiving step comprises:
receiving the pairing key at the client receiver, wherein the pairing key is encrypted; and
decrypting the pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

10

35. The method of claim 34, further comprising:
receiving the pairing key at the conditional access module; and
transferring the pairing key from the conditional access module to the client receiver.

15

36. The method of claim 31, wherein the transferring step comprises:
transferring the re-encrypted media encryption key from the conditional access module to the host receiver;
receiving the re-encrypted media encryption key from the conditional access module at the host receiver; and
20 transferring the re-encrypted media encrypted key from the host receiver to the client receiver.

25

37. The method of claim 36, further comprising
decrypting the re-encrypted media encryption key at the host receiver using a pairing key shared between the conditional access module and the host receiver, wherein the pairing key shared between the conditional access module and the host receiver is the same as the pairing key shared between the conditional access module and the client receiver; and

30

decrypting the encrypted program materials at the host receiver using the decrypted media encryption key.

38. An apparatus for distributing program materials received from a broadcast system between a host and client receiver for remote decryption, comprising:

5 (a) means for receiving an encrypted media encryption key at a conditional access module associated with the host receiver;

(b) means for decrypting the encrypted media encryption key at the conditional access module;

10 (c) means for re-encrypting the decrypted media encryption key at the conditional access module using a pairing key shared between the conditional access module and the client receiver;

(d) means for transferring the re-encrypted media encryption key from the conditional access module to the client receiver;

15 (e) means for decrypting the re-encrypted media encryption key at the client receiver using the pairing key shared between the conditional access module and client receiver;

(f) means for receiving encrypted program materials from the broadcast system at the host receiver;

(g) means for transferring encrypted program materials from the host receiver to the client receiver; and

20 (h) means for decrypting the encrypted program materials at the client receiver using the decrypted media encryption key.

39. The apparatus of claim 38, further comprising means for receiving the pairing key from the broadcast system at both the conditional access module and the client receiver.

40. The apparatus of claim 39, wherein the means for receiving comprises:
means for receiving the pairing key from the broadcast system at the conditional access module, wherein the pairing key is encrypted; and
30 means for decrypting the pairing key at the conditional access module.

41. The apparatus of claim 39, wherein the means for receiving comprises:
means for receiving the pairing key at the client receiver, wherein the pairing key
is encrypted; and

5 means for decrypting the pairing key at the client receiver using a receiver key
uniquely associated with the client receiver.

42. The apparatus of claim 41, further comprising:
means for receiving the pairing key at the conditional access module; and
means for transferring the pairing key from the conditional access module to the
10 client receiver.

43. The apparatus of claim 38, wherein the means for transferring comprises:
means for transferring the re-encrypted media encryption key from the conditional
access module to the host receiver;

15 means for receiving the re-encrypted media encryption key from the conditional
access module at the host receiver; and

means for transferring the re-encrypted media encrypted key from the host receiver
to the client receiver.

20 44. The apparatus of claim 43, further comprising
means for decrypting the re-encrypted media encryption key at the host receiver
using a pairing key shared between the conditional access module and the host receiver,
wherein the pairing key shared between the conditional access module and the host
receiver is the same as the pairing key shared between the conditional access module and
25 the client receiver; and

means for decrypting the encrypted program materials at the host receiver using
the decrypted media encryption key.